AUGMENTING SCALABLE CODING THROUGH VARIOUS BLOCK TRUNCATION CODING TECHNIQUES: IMPACTING ENCRYPTED IMAGES FOR SECURE DATA TRANSMISSION APPLICATIONS

A SYNOPSIS

Submitted by

P. JEYA BRIGHT

(Reg. No. 201708253)

in partial fulfilment for the award of the degree

of

DOCTOR OF PHILOSOPHY

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

SCHOOL OF ELECTRONICS, ELECTRICAL AND BIOMEDICAL TECHNOLOGY

KALASALINGAM ACADEMY OF RESEARCH AND EDUCATION

(DEEMED TO BE UNIVERSITY)

ANAND NAGAR, KRISHNANKOIL – 626 126

TAMILNADU, INDIA.

MAY 2023

1. INTRODUCTION

Scalable coding on encrypted images especially in encrypted signal processing has attracted more research interests in today's world, where processing of encrypted signals has emerged as a challenging research field. The signals such as audio, images and video are first compressed using various state-of-the-art compression techniques and then encrypted. In many applications, it is likable to carry out signal processing operations directly on encrypted signals. It is called as secure signal processing or signal processing in the encrypted domain. The relevance of carrying out signal manipulations using algorithm on encrypted signals is entirely dependent on the security requirements of the application scenario. The implementation of signal processing algorithm is determined by the possibilities and impossibilities of the cryptosystem employed. It is very likely that new requirements for cryptosystem will emerge from secure signal processing operations and applications. Hence, secure signal processing pose a joint challenge for both the signal processing and the cryptographic community.

Block Truncation Coding technique is a popular and most widely used algorithm for image processing applications due to its simplicity and parallel processing operation. This technique gives better PSNR, CR, MSE, and BR than other techniques. The computation time and memory size requirement are lower than any other techniques available today. The BTC algorithm primarily depends upon two-level quantizer and the principal content is reconstructed using these two-level quantizer. The scalable coding on encrypted signals is carried out using this BTC Technique. The scaling is done by scaling factor 2, and the popular image scaling technique namely Bilinear Interpolation technique is used.

2. LITERATURE REVIEW

Scalability on encrypted signals is an imperative research area that has attracted more interest in the signal processing community, and for secure transmission with low cost requires image encryption and compression, equally. The study about the challenges in signal processing by Erkin et al. [1] and the homomorphic properties of DFT and FFT are achieved by Bianchi et al. [2]. Troncoso and Perez-Gonzalez [3] have given importance to privacy protection on signal processing, and the size of encrypted signals is reduced by Bianchi et al. [4]. An invisible watermarking technique is

introduced by Memon and Wong [5], and the difficulty faced in using the watermarking technique is overcome by the fingerprinting technique proposed by Kuribayashi and Tanaka [6].

Today, image data storage requirement is very much higher, and the usage of image compression is inevitable. The traditional way of transmitting data is first compressing it and then encrypting it. But this process is reversed in Johnson et al. [7], Schonberg et al. [8], Lazzeretti and Barni [9], and Kumar and Makur [10], which is achieved by first encrypting it and then compressing it, where the encrypted key is not known to the compressor, and the principal content with originality is rebuilt by using joint decryption and decompression. Lazzeretti and Barni [9], described that instead of sparse black and white images, color images can be used, and in Kumar and Maku [10], a compressive sensing technique is used for image compression. Zhang [11], proposed that the raw image is first encrypted by pseudo-random permutation, then compressed into fine and excessive rough coefficients using orthogonal transform, and then the principal content is rebuilt using an iterative updating procedure.

Most of the applications use scalability, and it refers to the manipulation of bitstreams to achieve the desired image quality. Rate Scalability converts a lower bit rate into a higher bit rate. Resolution Scalability converts lower resolution into higher resolution. Scalable coding on unencrypted images is carried out by Bilgin et al. [12] and Taubman [13]. The desired scalability in terms of either rate scalability or resolution scalability was achieved in Bilgin et al. [12], and the raw image is compressed using reversible wavelet transform and encoded as embedded bitstreams. A compression algorithm, namely Embedded Block Coding with Optimized Truncation of the embedded bitstreams (EBCOT) is used in Taubman [13], and both resolution and SNR scalabilities are achieved through this.

The Scalable coding for processing the encrypted images is done in Xinpeng et al. [14], in which raw image is encrypted first, Hadamard transform is used for image compression, and the reconstruction of principal content is achieved using scaling technique. The BTC technique was used for image compression and image reconstruction in Edward and Robert [15]. It has poor rebuilt image quality, where PSNR and CR are lower, and higher bit error rate occur. The AMBTC technique was used for image compression and image reconstruction in Maximo and Robert [16]. It

has improved rebuilt image quality, PSNR, CR and bit error rate than BTC. The MBTC technique was used for image compression and image reconstruction in Jayamol et al. [17]. It has improved rebuilt image quality, PSNR, CR and bit error rate than BTC and AMBTC. MBTC technique is widely used in applications, such as internet video, digital cameras and printers. MBTC technique provides reduced storage space and supports parallel processing. The scalable coding for encrypted images was carried out using DMMBTC in Pankiraj et al. [18], where the raw image compression is achieved using DMMBTC, encrypted by PRN, decrypted by PRN key and then the principal content is reconstructed using DMMBTC and Scaling techniques. The proposed DMMBTC technique gives better PSNR, wPSNR, CR, BR, MSE, wMSE, Computational Time and Memory Size requirement than the existing Xinpeng et al. [14], Edward and Robert [15], Maximo and Robert [16] and Jayamol et al. [17].

The scalable coding for encrypted images was carried out using BTC in Jeya Bright and Vishnuvarthanan [19], especially for raw image compression, encrypted and decrypted through PRN key, and then reforming the same was done using BTC and Scaling techniques. The proposed technique gives better PSNR, wPSNR, CR, BR, MSE, wMSE, Computational Time and Memory Size requirement than the existing Xinpeng et al. [14], Edward and Robert [15], Maximo and Robert [16], Jayamol et al. [17] and Pankiraj et al. [18]. The scalable coding for encrypted images was carried out using BTC for different non-overlapping block sizes in Pankiraj et al. [20], and the experimental results of PSNR, wPSNR, CR, BR, MSE, wMSE, Computational Time and Memory Size shows that non-overlapping block size of 4×4 is the best for all image processing application. The scalable coding for encrypted images was carried out using EBTC technique in Pankiraj et al. [21], where the input image is compressed using EBTC technique and then encrypted using pseudo-random number. At the receiver side, the transmitted data is first decrypted by the shared pseudo-random number and then the principal content is reconstructed by the two-level quantizer of EBTC. The proposed technique gives better PSNR, wPSNR, CR, BR, MSE, wMSE, Computational Time and Memory Size requirement than the existing Xinpeng et al. [14], Edward and Robert [15], Maximo and Robert [16], Jayamol et al. [17], Pankiraj et al. [18] and Jeya Bright and Vishnuvarthanan [19].

Pankiraj et al. [22] proposes a novel method of scalable coding for encrypted images using the MDMMBTC, which has not been yet reported. MDMMBTC compresses the gray image, encrypted by PRN and transmitted. By using PRN, the transmitted image is decrypted at the receiver. Finally, the original content is rebuilt with the help of MDMMBTC and image scaling technique. The proposed technique gives better PSNR, wPSNR, CR, BR, MSE, wMSE, Computational Time and Memory Size requirement than the existing Xinpeng et al. [14], Edward and Robert [15], Maximo and Robert [16], Jayamol et al. [17], Pankiraj et al. [18], Jeya Bright and Vishnuvarthanan [19] and Pankiraj et al. [21].

3. OBJECTIVES

The main objectives of the research are as follows:

I. To develop scalable coding for the encryption of images using Diagonal Min-Max Block Truncation Code.
II. To develop scalable coding for the encryption of images using Block Truncation Code.
III. To develop scalable coding on encrypted images using Block Truncation Code for different block size.
IV. To develop scalable coding for the encryption of images using Enhanced Block Truncation Code.
V. To develop scalable coding for the encryption and decryption of images using Modified Diagonal Min-Max Block Truncation Code.

4. RESEARCH PROBLEM

Scalable coding on encrypted domains is essentially needed for secured signal transmission with low time-cost. The algorithm used should have low computational complexity, low storage requirement and better PSNR, wPSNR, CR, and lower values of BR, MSE and wMSE. BTC technique is most popular and widely used technique for all image processing applications due to its low storage requirement and low computational complexity. BTC uses two-level quantizer for image compression and image reconstruction. By modifying the two-level quantizer, optimized performance

can be achieved in terms of PSNR, wPSNR, CR, and lesser values of BR, MSE, wMSE, Computational Time and Memory Size requirement.

5. CONTRIBUTIONS

5.1 Development of a Scalable Coding for the encryption of images using Diagonal Min-Max Block Truncation Code

The proposed algorithm uses two-level quantizer as diagonal maximum value and diagonal minimum value of each non-overlapping block, and hence it is named as DMMBTC. The input image is first compressed by using DMMBTC technique, then encrypted by using pseudo-random number (PRNG) and then transmitted. The PRNG is shared to the receiver side, wherein it is first decrypted by PRNG, and then the principal content is reconstructed in three stages. In the first stage, it is reconstructed by the two-level quantizer of DMMBTC namely diagonal maximum value and diagonal minimum value of each non-overlapping block, then secondly, scaled by scaling factor 2, and finally, the principal content is reconstructed to its original image size using bilinear interpolation technique. Figure 1(a) shows the original image, Figure 1(b) shows the reconstructed image and Figure 2 shows the comparison between the existing technique Hadamard and proposed DMMBTC. The performance measures obtained from the proposed method is illustrated in Table 1.

Figure 1(a). Original Image

Figure 1(b). Reconstructed Image

(a)

(b)

Figure 2. Comparison between existing technique Hadamard and proposed technique DMMBTC (a) Hadamard (b) DMMBTC

Table 1. Performance measures of DMMBTC method

INPUT IMAGE	CR in %	BR in bpp	MSE in %	wMSE in %	PSNR in dB	wPSNR in dB	Computational Time in Seconds	Memory Size in MB
Lena	0.84	3.06	60.10	0.0075	30.34	69.40	7.56	1433
Cameraman	0.85	3.01	74.32	-	29.42	-	7.06	1421
Pout	0.93	2.75	6.19	0.0004	40.21	81.84	7.43	1427
Rice	0.88	2.92	47.27	0.0037	31.38	72.45	7.21	1430
Football	1.07	2.39	29.23	0.0041	33.47	72.04	7.04	1424
Peppers	1.09	2.35	28.95	0.0042	33.51	71.95	8.63	1412

5.2 Development of a Scalable Coding for the Encryption of images using Block Truncation Code

The proposed method uses two-level quantizer as mean value and variance value of each non-overlapping block. The input image is first compressed by using BTC technique, then encrypted by using pseudo-random number (PRNG) and then transmitted. The PRNG is shared to the receiver side, whereof the first decryption takes place through PRNG and then the principal content is reconstructed in three stages. In the first stage, it is reconstructed by the two-level quantizer of BTC, namely p and q, which are calculated through mean value and variance value of each non-overlapping blocks, then secondly, scaled by scaling factor 2, and finally, the principal content is reconstructed to its original image size using bilinear interpolation technique. Figure 3(a) shows the original image, Figure 3(b) shows the reconstructed image and Figure 4 shows the existing techniques of Hadamard and DMMBTC compared to BTC. The performance measures obtained from the proposed method is illustrated in Table 2.

Figure 3(a). Original Image

Figure 3(b). Reconstructed Image

(a) **(b)** **(c)**

Figure 4. Comparison between existing technique Hadamard, DMMBTC and proposed technique BTC (a) Hadamard (b) DMMBTC (c) BTC

Table 2. Performance measures of BTC method

INPUT IMAGE	CR in %	BR in bpp	MSE in %	wMSE in %	PSNR in dB	wPSNR in dB	Computational Time in Seconds	Memory Size in MB
Lena	0.902	2.835	34.52	0.0042	32.7489	71.9452	11.8183	1624
Cameraman	0.887	2.887	37.43	0.0143	32.3985	66.5810	11.4777	1623
Pout	0.999	2.561	3.187	0.0002	43.0961	84.6481	11.5467	1630
Rice	0.907	2.823	23.81	0.0019	34.3626	75.3808	11.3831	1638
Football	1.098	2.329	16.59	0.0023	35.9305	74.4476	11.8647	1634
Peppers	1.186	2.157	15.21	0.0023	36.3091	74.5902	13.9388	1639

5.3 Development of Scalable Coding on Encrypted images using BTC for different Non-Overlapping Block Sizes

In the proposed method, the input image is divided into different non-overlapping block sizes, namely 2×2, 4×4, 8×8 and 16×16. Each non-overlapping block size undergoes the following processes. First it is compressed by using BTC technique, then encrypted by pseudo-random number and transmitted. At the receiver side, it is first decrypted by PRNG, and then the principal content is reconstructed in three stages. In the first stage, it is reconstructed by the two-level quantizer of BTC, namely p and q, which are calculated by mean and variance values of each non-overlapping block, then secondly scaled by scaling factor 2, and finally, the principal content is reconstructed to its original image size using bilinear interpolation technique. Figure 5 shows the comparison between the original image and the reconstructed image of different non-overlapping block sizes, namely 2×2, 4×4, 8×8 and 16×16. The performance measures obtained from the proposed method is illustrated in Table 3.

Figure 6 shows the comparison of various state-of-art techniques with the different non-overlapping block sizes, namely 2×2, 4×4, 8×8 and 16×16.

(a) **(b)** **(c)** **(d)** **(e)**

Figure 5. Comparison between original content and reconstructed content (a) Original content (b) Reconstructed Content (2×2) (c) Reconstructed Content (4×4) (d) Reconstructed Content (8×8) (e) Reconstructed Content (16×16)

Table 3. Performance measures for different N.O.B sizes 2×2, 4×4, 8×8 and 16×16

INPUT IMAGE	Block Size	CR in %	BR in bpp	MSE in %	wMSE in %	PSNR in dB	wPSNR in dB	Computational Time in Seconds	Memory Size in MB
Cameraman	2×2	0.9665	2.6487	6.6593	-	39.8965	-	28.9413	1511
	4×4	0.8866	2.8874	37.4309	0.0143	32.3985	66.581	9.9835	1477
	8×8	0.8363	3.0611	92.2058	0.0277	28.4832	63.7035	5.9444	1476
	16×16	0.8039	3.1845	153.628	0.0433	26.2661	61.7655	3.9282	1472
Pout	2×2	0.9865	2.5949	0.6193	0.00004	50.2121	91.747	34.8874	1500
	4×4	0.9996	2.5611	3.1876	0.0002	43.0961	84.6481	11.395	1465
	8×8	0.885	2.8928	9.4014	0.0006	38.3989	80.0609	5.1578	1487
	16×16	0.8372	3.0578	19.9387	0.0014	35.1338	76.7584	3.9526	1479
Rice	2×2	0.9786	2.6161	5.0937	0.0003	41.0604	82.379	28.588	1499
	4×4	0.9067	2.8235	23.8134	0.0019	34.3626	75.3808	9.9613	1461
	8×8	0.8404	3.0462	58.5768	0.0045	30.4684	71.6234	5.4452	1481
	16×16	0.8264	3.0977	101.755	0.0076	28.0552	69.2944	4.0127	1476
Football	2×2	1.0924	2.3435	3.6176	0.0004	42.5466	81.2097	28.6287	1503
	4×4	1.099	2.3294	16.597	0.0023	35.9305	74.4476	10.3069	1455
	8×8	1.0762	2.3787	32.2612	0.0045	33.044	71.6357	5.2384	1476
	16×16	1.0356	2.4719	47.1335	0.007	31.3975	69.6885	4.1263	1471
Peppers	2×2	1.2189	2.1003	3.3499	0.0004	42.887	81.3976	28.9197	1512
	4×4	1.1864	2.1578	15.2116	0.0023	36.3091	74.5902	9.9243	1462
	8×8	1.0808	2.3686	34.9015	0.0052	32.7024	70.9843	5.1247	1477
	16×16	1.0454	2.4487	79.5143	0.0116	29.1264	67.4875	3.9521	1474

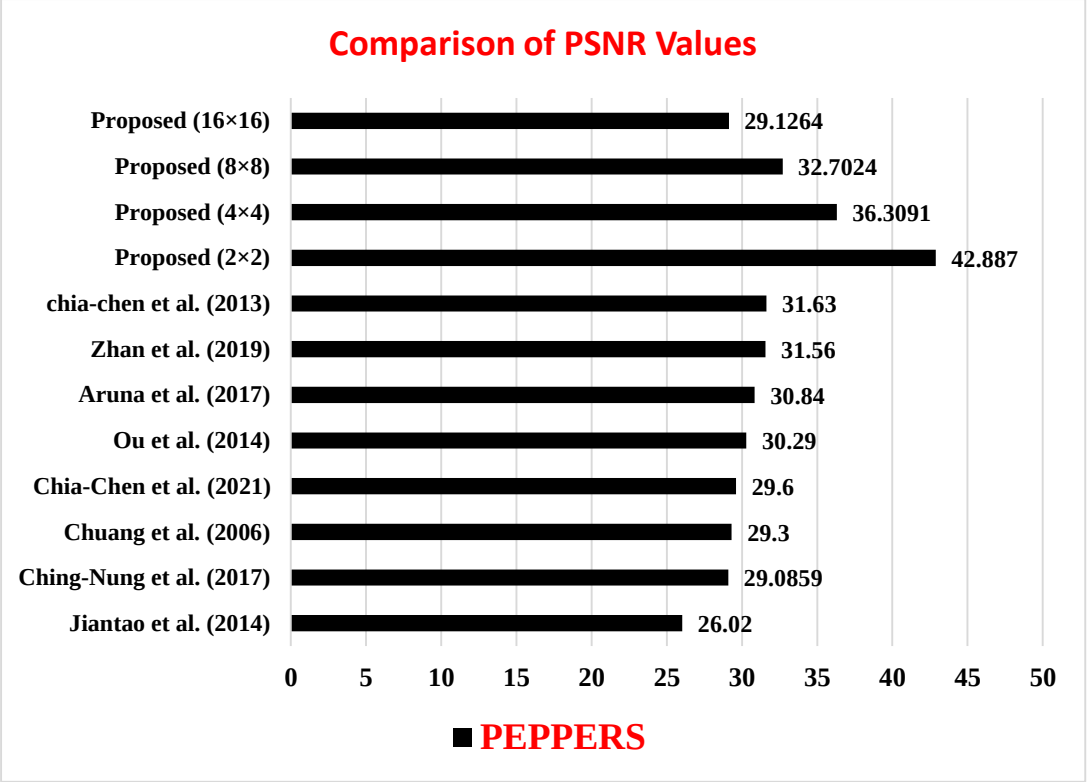

Figure 6. Comparison between various state-of-the-art techniques with the different N.O.B sizes 2×2, 4×4, 8×8 and 16×16. intended for image compression and decryption.

5.4 Development of scalable coding of encrypted images using Enhanced Block Truncation Code

The proposed method uses two-level quantizer as maximum prime value and minimum prime value of each non-overlapping blocks, and hence it is named as EBTC. The input image is first compressed by using EBTC technique, then encrypted by using pseudo-random number (PSRN), and then transmitted. The PSRN is shared to the receiver side, where the data is first decrypted by PSRN and then the principal content is reconstructed in three stages. In the first stage, the decrypted data is reconstructed by the two-level quantizer of EBTC, then secondly, scaled by scaling factor 2, and finally, the principal content is reconstructed to its original image size using bilinear interpolation technique. Figure 7 (a) shows the original image, Figure 7 (b) shows the reconstructed image, and Figure 8 shows the comparison between the existing Hadamard, DMMBTC, BTC techniques and the recommended EBTC technique. The performance measures obtained from the proposed method is illustrated in Table 4. Figure 9 shows the comparison of various state-of-art techniques with proposed method.

Figure 7(a). Original Image

Figure 7(b). Reconstructed Image

(a)

(b)

(c)

(d)

Figure 8. Comparison between existing technique Hadamard, DMMBTC, BTC and proposed technique EBTC (a) Hadamard (b) DMMBTC (c) BTC (d) EBTC

Table 4. Performance measures of EBTC method

INPUT IMAGE	CR in %	BR in bpp	MSE in %	wMSE in %	PSNR in dB	wPSNR in dB	Computational Time in Seconds	Memory Size in MB
Lena	1.0124	2.5287	33.681	0.004	32.856	72.1204	45.1593	1357
Cameraman	0.9845	2.6003	37.665	0.0139	32.371	66.6865	45.9858	1367
Pout	1.107	2.3127	3.5554	0.0002	42.621	84.0875	45.203	1370
Rice	0.9785	2.6162	23.546	0.0018	34.411	75.4706	44.7999	1370
Football	1.2237	2.092	15.918	0.0022	36.111	74.6414	44.664	1376
Peppers	1.2915	1.9822	14.794	0.0022	36.429	74.6829	58.2594	1271

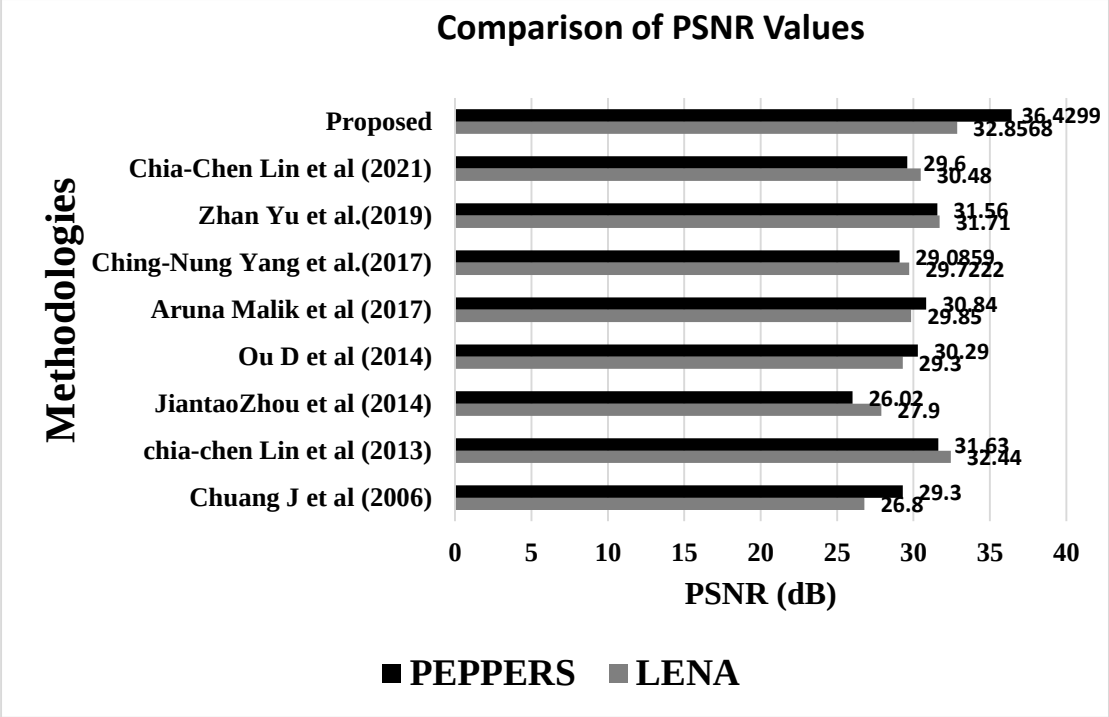

Figure 9. Comparison between various state-of-the-art techniques with the proposed system intended for image compression and decryption.

5.5 Development of scalable coding for the encryption and decryption of images using Modified Diagonal Min-Max Block Truncation Code.

In the proposed method, the input image is first compressed by using MDMMBTC technique, then encrypted by using pseudo-random number (PRN) and transmitted alas. The PRN is shared to the receiver side, where first-level decryption is done by PRN and then the principal content is reconstructed in three stages. In the first stage, the decrypted data is reconstructed by the two-level quantizer of MDMMBTC, then secondly, scaled by scaling factor 2 and finally, the principal content is reconstructed to its original image size using bilinear interpolation technique. Figure 10 (a) shows the original image, Figure 10 (b) shows the reconstructed image and Figure 11 shows the comparison between existing techniques like Hadamard, DMMBTC, BTC, EBTC with the MDMMBTC techniques. The performance measures obtained from the proposed method is illustrated in Table 5. The performance measures obtained from the proposed method is compared with existing techniques of Hadamard, DMMBTC, BTC and EBTC, which is illustrated in Table 6. Figure 12 shows the comparison of various state-of-art techniques with the proposed MDMMBTC technique.

Figure 10(a). Original Image

Figure. 10(b). Reconstructed Image

(a)

(b)

(c)

(d)

(e)

Figure 11. Comparison between existing technique Hadamard, DMMBTC, BTC, EBTC and proposed technique MDMMBTC (a) Hadamard (b) DMMBTC (c) BTC (d) EBTC (e) MDMMBTC

Table 5. Performance measures of MDMMBTC method

INPUT IMAGE	CR in %	BR in bpp	MSE in %	wMSE in %	PSNR in dB	wPSNR in dB	Computational Time in Seconds	Memory Size in MB
Lena	0.9978	2.5657	27.9588	0.0036	33.6656	72.5707	26.9728	1440
Cameraman	0.9548	2.6812	31.7436	0.0143	33.1142	66.5751	26.5185	1421
Pout	1.0818	2.3665	2.7896	0.0001	43.6754	85.2032	26.4086	1419
Rice	0.9731	2.6308	19.7083	0.0016	35.1843	76.0951	26.5897	1420
Football	1.2145	2.1079	13.9232	0.002	36.6934	75.1159	26.586	1418
Peppers	1.2854	1.9917	12.2228	0.002	37.2591	75.2125	26.7731	1412

Table 6. Comparison of performance measures of Hadamard, DMMBTC, BTC, EBTC and MDMMBTC Methods

INPUT IMAGE	Methodologies	CR in %	BR in bpp	MSE in %	wMSE in %	PSNR in dB	wPSNR in dB	Computational Time in Seconds	Memory Size in MB
Lena	Hadamard	0.6233	4.1072	386.74	0.0461	22.2566	61.4902	24.4201	1675
	DMMBTC	0.84	3.06	60.10	0.0075	30.34	69.40	7.56	1433
	BTC	0.902	2.835	34.52	0.0042	32.7489	71.9452	11.8183	1624
	EBTC	1.0124	2.5287	33.681	0.004	32.8568	72.1204	45.1593	1357
	MDMMBTC	0.9978	2.5657	27.958	0.0036	33.6656	72.5707	26.9728	1440
Cameraman	Hadamard	0.5312	4.8191	640.91	0.149	20.0628	56.3999	23.17	1678
	DMMBTC	0.85	3.01	74.32	-	29.42	-	7.06	1421
	BTC	0.8866	2.8874	37.430	0.0143	32.3985	66.581	9.9835	1477
	EBTC	0.9845	2.6003	37.665	0.0139	32.3714	66.6865	45.9858	1367
	MDMMBTC	0.9548	2.6812	31.743	0.0143	33.1142	66.5751	26.5185	1421
Pout	Hadamard	0.5741	4.4592	47.627	0.0037	31.3522	72.4125	21.9238	1683
	DMMBTC	0.93	2.75	6.19	0.0004	40.21	81.84	7.43	1427
	BTC	0.9996	2.5611	3.1876	0.0002	43.0961	84.6481	11.395	1465
	EBTC	1.107	2.3127	3.5554	0.0002	42.6219	84.0875	45.203	1370
	MDMMBTC	1.0818	2.3665	2.7896	0.00019	43.6754	85.2032	26.4086	1419
Rice	Hadamard	0.6142	4.1677	312.71	0.0254	23.1794	64.085	21.7094	1684
	DMMBTC	0.88	2.92	47.27	0.0037	31.38	72.45	7.21	1430
	BTC	0.9067	2.8235	23.813	0.0019	34.3626	75.3808	9.9613	1461
	EBTC	0.9785	2.6162	23.546	0.0018	34.4115	75.4706	44.7999	1370
	MDMMBTC	0.9731	2.6308	19.708	0.0016	35.1843	76.0951	26.5897	1420
Football	Hadamard	0.8443	3.0322	236.21	0.0237	24.3976	64.3902	21.6885	1696
	DMMBTC	1.07	2.39	29.23	0.0041	33.47	72.04	7.04	1424
	BTC	1.099	2.3294	16.597	0.0023	35.9305	74.4476	10.3069	1455
	EBTC	1.2237	2.092	15.918	0.0022	36.1117	74.6414	44.664	1376
	MDMMBTC	1.2145	2.1079	13.923	0.002	36.6934	75.1159	26.586	1418
Peppers	Hadamard	0.7206	3.5525	267.20	0.0356	23.8623	62.6117	21.5737	1700
	DMMBTC	1.09	2.35	28.95	0.0042	33.51	71.95	8.63	1412
	BTC	1.1864	2.1578	15.211	0.0023	36.3091	74.5902	9.9243	1462
	EBTC	1.2915	1.9822	14.794	0.0022	36.4299	74.6829	58.2594	1271
	MDMMBTC	1.2854	1.9917	12.222	0.002	37.2591	75.2125	26.7731	1412

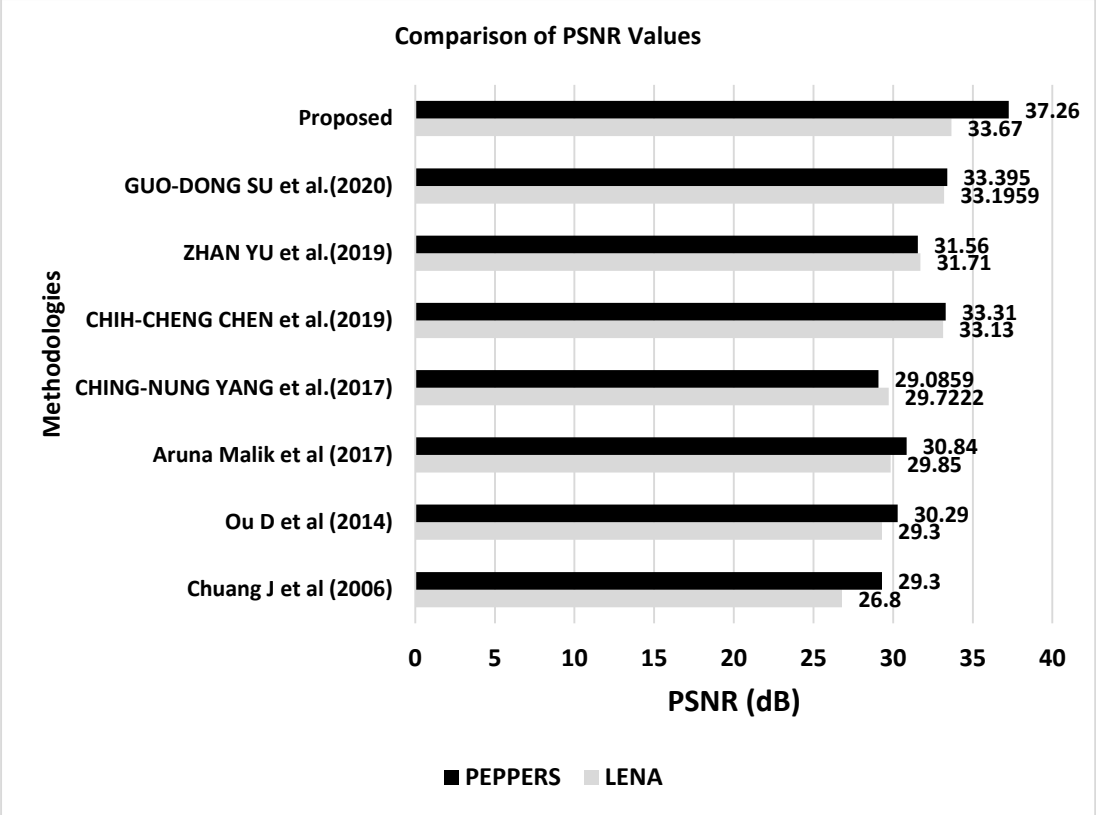

Figure 12. PSNR for various images using various state –of-the -art techniques intended for image compression and decryption

6. CONCLUSION

The proposed scalable coding on encrypted images using diagonal min-max block truncation code uses diagonal maximum value and diagonal minimum value of the non-overlapping block as two-level quantizer. The developed algorithms show improved performance metric parameters such as Compression Ratio, Bit Rate, PSNR, wPSNR, MSE, wMSE, Computational Time and Memory Size than the existing techniques of scalable coding on encrypted images using Hadamard Transform. Still there is space for improving performance metric parameters such as Compression Ratio, Bit Rate, PSNR, wPSNR, MSE, wMSE, Computational Time and Memory Size by pruning the two-level quantizer. This is achieved by scalable coding on encrypted images using block truncation code technique, where mean and variance value of the non-overlapping block is used to calculate the two-level quantizer. The developed algorithm shows improved performance metric parameters such as Compression Ratio, Bit Rate, PSNR, wPSNR, MSE, wMSE, Computational Time and Memory Size than the existing technique of scalable coding on encrypted images using Hadamard Transform and scalable coding on encrypted images using diagonal min-max block

truncation code. An analysis is done to figure out which non-overlapping block size is better, and it is done for different non-overlapping block sizes, namely 2×2, 4×4, 8×8 and 16×16 using Block Truncation Code. From the analysis it is figured that non-overlapping block size 4×4 is much suitable for all image processing applications. A new algorithm namely scalable coding on encrypted images using enhanced block truncation code is developed, which gives improved performance metric parameters such as Compression Ratio, Bit Rate, PSNR, wPSNR, MSE, wMSE, Computational Time and Memory Size than the existing technique for scalable coding of encrypted images using Hadamard Transform, scalable coding of encrypted images using diagonal min-max block truncation code and scalable coding on encrypted images using block truncation code. Yet, there is a wide opportunity available for further improvement of the above said values, which has been achieved through the development of scalable coding of encrypted images using modified diagonal min-max block truncation code technique. The developed scalable coding of encrypted images using Modified Diagonal Min-Max Block Truncation Code uses mean value, diagonal maximum value and diagonal minimum value of the non-overlapping block to calculate the threshold value and high range value and low range value of the non-overlapping blocks to calculate the two-level quantizer. Among the DMMBTC, BTC, EBTC and MDMMBTC algorithms developed through this research work, the MDMMBTC algorithm has better performance metric parameters such as Compression Ratio, Bit Rate, PSNR, wPSNR, MSE, wMSE, Computational Time and Memory Size within a limited time frame, making it to be the preferential one.

7. ORGANIZATION OF THE THESIS

The thesis is organized as follows: The significance of secured signal processing on encrypted images have been explained in Chapter 1. Chapter 2 provides a brief overview of unscalable coding on encrypted images and the issues regarding the secured signal processing on encrypted domain. This thesis's aspiration and scope are excessively described. Chapter 3 describes the scalable coding on encrypted images using diagonal min-max block truncation code algorithm and its improved performance than existing techniques.

Chapter 4 discusses the scalable coding on encrypted images using block truncation code algorithm, and it possesses better performance metrics than the

previous techniques. Chapter 5 explains the usage of non-overlapping block size 4×4 as the best suitable for any image processing application when compared to other non-overlapping block sizes, namely 2×2, 8×8 and 16×16. Chapter 6 discusses the scalable coding on encrypted images using EBTC technique, and it possesses better performance metrics than the previous techniques. Chapter 7 discusses the scalable coding on encrypted images using MDMMBTC technique, and it has better performance metrics than all other existing techniques. Chapter 8 concludes the research work and discusses the efforts made in this research study as well as the best algorithm for scalable coding on encrypted images is MDMMBTC technique among DMMBTC, BTC and EBTC techniques. The research work concludes with the revelation of considerable recommendation for future investigation. The references of all the hybrid algorithms that are employed for the scalable coding on encrypted images in this research work are enlisted.

8. REFERENCES

1. Z.Erkin, A.Piva, S.Katzenbeisser, R.L.Lagendijk, J.Shokrollahi, G.Neven and M.Barni, Protection and retrieval of encrypted multimedia content: When cryptography meets signal processing, *EURASIP Journal on Information Security*, 7894 (2007), pp 1-20.
2. T.Bianchi, A.Piva, and M.Barni, On the implementation of the discrete Fourier transform in the encrypted domain, *IEEE Transformation on Information Forensics and Security*, **4** (2009), 86–97.
3. J.R.Troncoso Pastoriza and F.Pérez-González, Secure adaptive filtering, *IEEE Transformation on Information Forensics and Security*, **6** (2) (2011), 469–485.
4. T.Bianchi, A.Piva and M.Barni, Composite signal representation for fast and storage-efficient processing of encrypted signals, *IEEE Transformation on Information Forensics and Security*, **5** (1) (2010), 180–187.
5. N.Memon and P.W.Wong, A buyer-seller watermarking protocol, *IEEE Transactions on Image Processing*, **10** (4) (2001), 643–649.
6. M.Kuribayashi and H.Tanaka, Fingerprinting protocol for images based on an additive homomorphic property, *IEEE Transactions on Image Processing*, **14** (12) (2005), 2129–2139.
7. M.Johnson, P.Ishwar, V.M.Prabhakaran, D.Schonberg and K.Ramachandran, On compressing encrypted data, *IEEE Transactions on Signal Processing*, **52** (10) (2004), 2992–3006.
8. D.Schonberg, S.C.Draper and K.Ramachandran, *On blind compression of encrypted correlated data approaching the source entropy rate*, Proceedings of 43rd Annual Allerton Conference, Allerton, IL, (2005).
9. R.Lazzeretti and M.Barni, *Lossless compression of encrypted grey level and color images*, Proceedings of 16th European Signal Processing Conference, Lausanne, Switzerland, (2008), 1-5.
10. A.Kumar and A.Makur, *Lossy compression of encrypted image by compressing sensing technique*, Proceedings of IEEE Region 10 conf (TENCON 2009), (2009), 1-6.
11. X.Zhang, Lossy compression and iterative reconstruction for encrypted image, *IEEE Transformation on Information Forensics and Security*, **6** (1) (2011), 53–58.

12. A.Bilgin, P.J.Sementilli, F.Sheng, and M.W.Marcelin, Scalable image coding using reversible integer wavelet transforms, *IEEE Transactions on Image Processing*, **9** (11) (2000), 1972–1977.
13. D.Taubman, High performance scalable image compression with EBCOT, *IEEE Transactions on Image Processing*, **9** (7) (2000), 1158–1170.
14. Xinpeng Zhang, Guorui Feng, Yanli Ren and Zhenxing Qian, Scalable Coding of Encrypted Images, *IEEE Transactions on Image Processing*, **21** (6) (2012), 3108-3114.
15. Edward J. Delp and O.Robert Mitchell, Image Coding Using Block Truncation Coding, *IEEE Transactions on Communications*, **27** (9) 1979, 1335-1342.
16. Maximo D. Lema and O Robert Mitchell, Absolute Moment Block Truncation Coding and its Application to color images, *IEEE Transactions on Communications*, **COM-32** (10) (1984), 1148-1157
17. Jayamol Mathews, Madhu S Nair and Liza Jo, *Modified BTC Algorithm for Gray Scale Images using max-min Quantizer*, Proceedings of Int. Multi Conference on Automation, Computing, Communication, Control and Compressed Sensing (iMac4s), Kottayam, India, (2013), 377-382.
18. Pankiraj Jeya Bright, Govindaraj Vishnuvarthanan., Murugan Pallikonda Rajasekaran and Thiyagarajan Arun Prasath, Development of a scalable coding for the encryption of images using Diagonal Min-Max Block Truncation Code, *International Journal of Engineering and Advanced Technology (IJEAT)*, **9** (IS4) (2019), 718-723.
19. P.Jeya Bright and G.Vishnuvarthanan, *Development of a scalable coding for the encryption of Images using Block Truncation Code*, Proc.3rd Int. Conf. Trends in Electronics and Informatics (ICOEI 2019), Tirunelveli, India, (2019), 934-938.
20. Pankiraj Jeya Bright, Govindaraj Vishnuvarthanan., Yudong Zhang., Murugan Pallikonda Rajasekaran and Ramaraj Kottaimalai, Development of scalable coding on Encrypted Images using BTC for different Non-overlapping Block Size, *Journal of signal, image and Video processing*, (2023).
21. Pankiraj Jeya Bright, Govindaraj Vishnuvarthanan., Yudong Zhang., Murugan Pallikonda Rajasekaran and Milton Anisha, Development of a scalable coding of encrypted images using Enhanced Block Truncation Code, *Webology*, 1**9** (1) (2022), 1620-1639.

22. Pankiraj Jeya Bright, Govindaraj Vishnuvarthanan., Yudong Zhang., Murugan Pallikonda Rajasekaran and Milton Anisha, Development of scalable coding for the encryption and decryption of images using Modified Diagonal Min-Max Block Truncation Code, *Multimedia Tools and Application*, **82** (8) (2023), 12263-12277.

List of Publications

1. Pankiraj Jeya Bright and Govindaraj Vishnuvarthanan, Development of a scalable coding for the encryption of Images using Block Truncation Code, *3rd International Conference on Trends in Electronics and Informatics* (ICOEI 2019), Tirunelveli, India, (2019), 934-938.
2. Pankiraj Jeya Bright, Govindaraj Vishnuvarthanan, Yudong Zhang, Murugan Pallikonda Rajasekaran and Milton Anisha, Development of scalable coding for the encryption and decryption of images using Modified Diagonal Min-Max Block Truncation Code, *Multimedia Tools and Application*, **82** (8) (2023), 12263-12277.
3. Pankiraj Jeya Bright, Govindaraj Vishnuvarthanan, Yudong Zhang, Murugan Pallikonda Rajasekaran and Ramaraj Kottaimalai, Development of scalable coding on Encrypted Images using BTC for different Non-overlapping Block Size, *Journal of signal, image and Video processing*, (2023).